

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-074221

(43)Date of publication of application : 17.03.1998

(51)Int.Cl.

G06F 17/60  
G06F 13/00  
G06F 19/00  
H04L 29/06

(21)Application number : 08-230288

(71)Applicant : DIGITAL VISION LAB:KK

(22)Date of filing : 30.08.1996

(72)Inventor : MUTO AKIHIRO

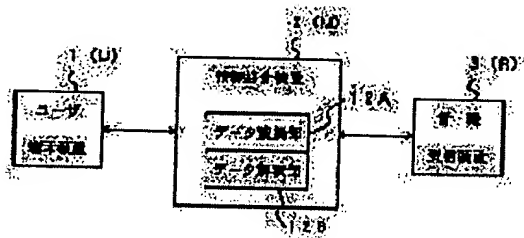
(54) INFORMATION MEDIATING DEVICE APPLIED TO NETWORK SYSTEM AND INFORMATION TRANSFER PROCESSING METHOD APPLIED TO THE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information mediating device capable of protecting user's privacy against an information receiving side and guaranteeing the reliability of information communication by preventing information or attribute data specified by a user from being disclosed to the information receiving side and securing the reliability of the user and transmitting information.

SOLUTION: An information mediating device 2 is used for a computer network such as an interconnection network and provided with a function capable of securing especially the anonymity of an information transmitting side and guaranteeing the reliability of the information transmitting side. Specifically, the device 2 includes a data interpreting part 12B for receiving information transmitting from an information transmitting equipment 1 and recognizing specified contents from the equipment 1 and a data converting part 12A for converting the originating source address of the equipment 1 into the address of the device 2. The data converting part 12A executes the data converting processing of the originating source address to be specific data not to be disclosed in accordance with the interpreted result of the interpreting part 12B.

Best Available Copy



## LEGAL STATUS

[Date of request for examination] 17.02.1998

[Date of sending the examiner's decision of rejection] 24.11.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-74221

(43) 公開日 平成10年(1998) 3月17日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21	3 3 0
13/00	3 5 1		13/00	3 5 1 Z
19/00			15/24	1 0 1
H 0 4 L 29/06			H 0 4 L 13/00	3 0 5 B

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21) 出願番号 特願平8-230288

(22) 出願日 平成8年(1996) 8月30日

(71) 出願人 396001360

株式会社デジタル・ビジョン・ラボラトリーズ

東京都港区赤坂七丁目3番37号

(72) 発明者 武藤 明宏

東京都港区赤坂七丁目3番37号 株式会社  
デジタル・ビジョン・ラボラトリーズ内

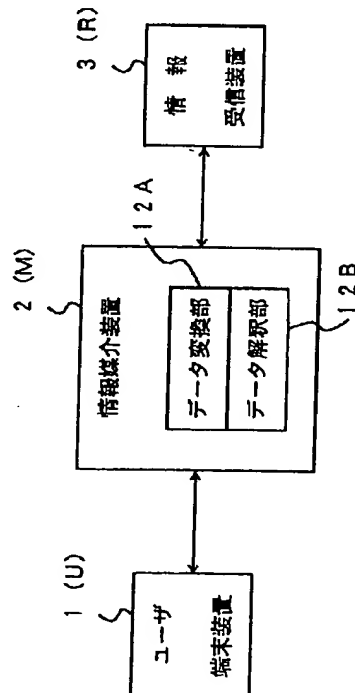
(74) 代理人 弁理士 鈴江 武彦 (外5名)

(54) 【発明の名称】 ネットワークシステムに適用する情報媒介装置及び同システムに適用する情報転送処理方法

## (57) 【要約】

【課題】 ユーザが指定した情報や属性データを情報受信側には非公開にし、かつユーザや送信情報の信頼性を確保できるようにして、情報受信側に対するユーザのプライバシーを保護すると共に、情報通信の信頼性を保証することが可能な情報媒介装置を提供することにある。

【解決手段】 例えばインターネットなどのコンピュータネットワークに使用される情報媒介装置2であり、特に情報発信側の匿名性を確保し、かつ情報発信側の信頼性を保証できる機能を備えた情報媒介装置である。具体的には、情報媒介装置2は、情報発信装置から発信された情報を受信して情報発信装置1からの指示内容を認識するためのデータ解釈部12Bと、情報発信装置1の発信元アドレスを情報媒介装置2のアドレスに変換するデータ変換部12Aとを有する。データ変換部12Aはデータ解釈部12Bの解釈結果に従って、非公開にすべき特定データである発信元アドレスのデータ変換処理を実行する。



## 【 特許請求の範囲】

【 請求項1 】 ネットワークに接続された情報発信装置と情報受信装置間に介在して、前記情報発信装置から発信された情報を前記情報受信装置に転送する情報媒介装置であって、

前記情報発信装置から発信された情報を受信して保存するデータ受信手段と、

前記データ受信手段により受信された情報から、前記情報発信装置からの指示内容を含む共有データを分離し、前記指示内容を認識する認識手段と、

前記指示内容に従って、前記受信された情報に含まれるデータであって前記情報受信装置に送信すべき本体データを除いて前記情報発信装置を識別するためのデータを所定のデータに変換するデータ変換手段と、

前記本体データと前記データ変換手段により変換されたデータとを含む情報を前記情報受信装置に送信する送信手段とを具備したことを特徴とする情報媒介装置。

【 請求項2 】 前記情報発信装置から発信される情報は、前記情報受信装置に送信すべき本体データと、前記情報媒介装置にデータ変換処理を含むデータ処理の内容を指示するための指示内容を含む共有データと、前記情報発信装置の送信元アドレスを含む特定データとから構成されており、

前記データ変換手段は、前記指示内容に含まれるデータ変換指示に従って、前記情報発信装置の送信元アドレスを前記情報媒介装置自体の送信元アドレスに変換することを特徴とする請求項1記載の情報媒介装置。

【 請求項3 】 前記データ変換手段は、前記指示内容に含まれるデータ変換指示に従って、前記特定データの中で前記送信元アドレスと共に前記情報発信装置を識別可能なデータを前記情報媒介装置自体の送信元アドレスを含む所定のデータに変換し、または前記特定データの全てを前記情報媒介装置自体の送信元アドレスを含む所定のデータに変換することを特徴とする請求項2記載の情報媒介装置。

【 請求項4 】 前記共有データは、前記指示内容をスクリプト言語により記述されたスクリプトデータを含み、前記認識手段は、前記スクリプト言語を解釈した結果により前記指示内容を認識する機能を備えたことを特徴とする請求項1記載の情報媒介装置。

【 請求項5 】 ネットワークに接続された情報発信装置と情報受信装置間に介在して、前記情報発信装置から発信された情報を前記情報受信装置に転送する情報媒介装置であって、

前記情報発信装置から発信された情報であって、前記情報受信装置に送信すべき本体データと、前記情報媒介装置にデータ変換処理を含むデータ処理の内容を指示するための指示内容を含む共有データと、前記情報発信装置の送信元アドレスを含む特定データとから構成された情報を受信する受信手段と、

前記受信手段により受信された情報を格納するデータバッファ手段と、

前記データバッファ手段により格納された情報から前記共有データを分離し、前記共有データから前記指示内容を解釈するデータ解釈手段と、

前記データ解釈手段により解釈された指示内容に従って、前記特定データに含まれるデータであって前記情報発信装置を識別するための送信元アドレスまたは送信元アドレスと共に前記情報発信装置を識別可能なデータを前記情報媒介装置自体のアドレスまたは前記情報媒介装置自体のアドレスを含む所定のデータに変換するデータ変換手段と、

前記データ解釈手段により解釈された指示内容に従って、前記データ変換手段により変換された前記情報媒介装置自体のアドレスを送信元アドレスとして、前記本体データを前記情報受信装置に送信する送信手段とを具備したことを特徴とする情報媒介装置。

【 請求項6 】 前記共有データは前記指示内容をスクリプト言語により記述されたスクリプトデータを含み、前記データ変換手段のアドレス変換処理の指示内容以外に、各種のサービス処理の指示内容を含み、

前記データ解釈手段は前記スクリプト言語の解釈により前記指示内容を認識する機能を有し、

前記データ解釈手段により解釈されたサービス処理の指示内容に従って、前記サービス処理に対応するアプリケーションソフトウェアを実行するサービス処理手段を備えていることを特徴とする請求項4記載の情報媒介装置。

【 請求項7 】 前記サービス処理の指示内容には、前記情報受信装置に送信した前記本体データに対する応答処理を要求する内容を含み、

前記データ解釈手段により解釈されたサービス処理の指示内容に従って、前記情報受信装置に前記応答処理の要求を実行し、前記情報受信装置からの応答データを前記情報発信装置に転送する応答処理手段を具備したことを特徴とする請求項5記載の情報媒介装置。

【 請求項8 】 ネットワークに接続された情報発信装置と情報受信装置間に介在して、前記情報発信装置から発信された情報を前記情報受信装置に転送する情報媒介装置の情報転送処理方法であって、

前記情報発信装置から発信された情報であって、前記情報受信装置に送信すべき本体データと、前記情報媒介装置にデータ変換処理を含むデータ処理の内容を指示するための指示内容を含む共有データと、前記情報発信装置の送信元アドレスを含む特定データとから構成された情報を受信するステップと、

受信した情報をデータバッファ手段に格納するステップと、

前記データバッファ手段により格納された情報から前記共有データを分離し、前記共有データから前記指示内容

を解釈するステップと、

解釈した前記指示内容に従って、前記特定データに含まれる前記情報発信装置を識別するためのデータを所定のデータに変換するステップと、

解釈した前記指示内容に従って、変換して得られた前記データを付加した前記本体データを前記情報受信装置に転送するステップとからなることを特徴とする情報転送処理方法。

【請求項9】 前記解釈した前記指示内容に従って前記情報発信装置を識別するためのデータを所定のデータに変換するステップにおいて、

前記情報発信装置を識別するためのデータとして、前記特定データに含まれるデータであって前記情報発信装置の送信元アドレスまたは前記送信元アドレスを含む前記情報発信装置を識別可能なデータを、前記情報媒介装置のアドレスまたは前記情報媒介装置のアドレスを含む所定のデータに変換することを特徴とする請求項8記載の情報転送処理方法。

【請求項10】 ネットワークに接続された情報発信装置と情報受信装置間に介在して、前記情報発信装置から発信された情報を前記情報受信装置に転送する情報媒介装置に設けられたコンピュータにより読取り可能な記憶媒体であって、

前記情報発信装置から受信した情報に含まれる前記情報受信装置に送信すべき本体データと、前記情報媒介装置にデータ変換処理を含む各種のサービス処理の指示内容をスクリプト言語により記述されたスクリプトデータと、前記情報発信装置の送信元アドレスを含む特定データとから前記スクリプトデータを分離し、前記指示内容を解釈する処理と、

前記指示内容の解釈結果に従って、前記特定データに含まれる前記情報発信装置を識別するための送信元アドレスを含むデータを前記情報媒介装置自体のアドレスを含む所定のデータに変換する処理と、

前記指示内容の解釈結果に従って、変換して得られた前記情報媒介装置自体のアドレスを送信元アドレスとして、前記本体データを前記情報受信装置に転送する処理と、

前記指示内容の解釈結果に従って、指定されたサービス処理に対応するアプリケーションソフトウェアを実行する処理とを前記コンピュータが実行するように設定されたプログラムを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばインターネットなどのコンピュータネットワーク上において、情報発信側と情報受信側との情報通信を媒介する装置であって、特に情報発信側の匿名性や特定情報の秘密性を保証するための機能を備えた情報媒介装置に関する。

【0002】

【従来の技術】近年、インターネットなどのコンピュータネットワークの発展により、各種の情報サービス以外に、映像などの付加価値の高い情報を含む商品の提供サービスがネットワーク上で実現されつつある。具体的には、ユーザの要求に応じた映像を提供するビデオ・オン・デマンドサービスや、インターネット上に構築されたショッピングモールなどに商品の照会や注文に応ずるサービスシステムが開発されている。

【0003】インターネットなどのコンピュータネットワークでは、ユーザはパーソナルコンピュータなどの端末装置を操作して、サービスを要求するための情報を、サービス提供者側(情報受信側)に送信することになるが、情報媒介装置を介して情報の送受信がなされる。この情報媒介装置は、情報中継装置やインターネット・プロバイダ(インターネット接続業者)に相当し、また必ずしも専用の業者やシステムには限定されず、ユーザが兼用する場合も含む広い概念である。

【0004】ところで、ネットワーク上において、ユーザが例えばショッピング・モールなどに商品照会の情報を送信するときに、商品照会の内容を記述した本体データ(電子メールの本文データに相当)以外に、送信情報には必然的に付加される情報がある。具体的には、インターネットなどで使用されるアドレス(例えばIPアドレスの送信元と宛先の各アドレス)を含むヘッダエリアのデータや電子メールの本文以外のヘッダ部分である。このようなアドレスなどのユーザを識別できる情報は、ユーザの個人的なプライバシー(privacy)に関する情報である。

【0005】従来では、ユーザの商品照会のように、必ずしも個人的なプライバシー情報を公開する必要がない情報通信の場合でも、ユーザの意思とは無関係に、アドレスのような個人的なプライバシー情報が情報提供者側に通知されることになる。このため、ユーザのアドレスなどの個人的情報が、例えば顧客リストの作成などの目的に流用されるなど、ユーザのプライバシーが侵害される可能性が高い。

【0006】

【発明が解決しようとする課題】従来のインターネットなどのネットワーク上の情報通信では、ユーザの意思とは無関係に、アドレスなどのユーザの個人的なプライバシー情報が公開される可能性が高く、ユーザのプライバシーを保護することは困難である。

【0007】一方、情報発信者のアドレスなどの属性データを非公開にして、情報発信者の匿名性を保証する情報通信システムでは、情報発信者及び発信データの信頼性がほとんど保証されない通信しかできないことになる。具体的には、通常の電話サービスがそれに相当する。また、匿名性を利用したいいわゆるネットワーク犯罪(マネーロンダリングなど)を増長させる要因になるなどの問題がある。

【0008】本発明の目的は、ユーザが指定した情報や属性データを情報受信側には非公開にし、かつユーザや送信情報の信頼性を確保できるようにして、情報受信側に対するユーザのプライバシーを保護すると共に、情報通信の信頼性を保証することが可能な情報媒介装置を提供することにある。

【0009】

【課題を解決するための手段】本発明は、例えばインターネットなどのコンピュータネットワークに使用される情報媒介装置であり、特に情報発信側の匿名性を確保し、かつ情報発信側の信頼性を保証できる機能を備えた情報媒介装置である。具体的には、情報媒介装置は、情報発信装置から発信された情報を受信して保存するデータ受信手段と、情報発信装置からの指示内容を認識する認識手段と、情報発信装置を識別するためのデータを所定のデータに変換するデータ変換手段と、情報を情報受信装置に送信する送信手段とを有する。

【0010】データ受信手段が受信する情報には、情報発信装置から情報受信装置に送信すべき本体データと、情報発信装置からの指示内容を含む共有データと、情報発信装置を識別するためのデータ(特定データ)とが含まれている。認識手段は、共有データを抽出して、情報発信装置からの指示内容を認識する。データ変換手段は、その指示内容に従って、特定データである例えばアドレスデータを情報媒介装置自体のアドレスデータに変換する。送信手段は、変換されたアドレスデータと共に、情報発信装置からの本体データを送信する。

【0011】このような構成により、第1に情報受信装置側には、情報発信者のアドレスではなく、情報媒介装置のアドレスが本体データと共に送信されるため、情報発信者のアドレスが情報受信側および情報発信側を介した第3者に公開されるような自体を防止することができる。換言すれば、情報発信者の匿名性を確保することができる。第2に、情報媒介装置は情報発信者のアドレスなどの特定データ、本体データ、共有データの全てまたは一部を受信して保存することにより、情報受信側に対して情報発信者の信頼性を保証することが可能である。さらに、第3として、共有データに前記のデータ変換処理などのサービス処理の指示内容を含ませることにより、情報媒介装置はその指示内容を認識して、例えば情報受信装置から送信した本体データに対する応答データを情報発信装置に転送するようなサービス処理を実行することができる。

【0012】

【発明の実施の形態】以下図面を参照して本発明の実施の形態を説明する。図1は本実施形態に係るシステム構成を示すブロック図であり、図2は本実施形態に係る情報媒介装置の構成を示すブロック図であり、図3と図4は本実施形態に係るデータ構造を説明するための概念図であり、図5は本実施形態の動作を説明す

るためのフローチャートであり、図6は本実施形態の動作を説明するための概念図である。

(システム構成)本システムは、インターネットなどのコンピュータネットワークを想定し、このネットワークに接続された情報送信装置1(U)と、情報媒介装置2(M)と、情報受信装置3(R)とを有する。本実施形態では、便宜的に情報送信装置1(U)は、情報発信者であるユーザが操作するユーザ端末装置として想定し、応答データ以外の情報の受信機能については除外される。同様に、情報受信装置3(R)は、後述するように、例えばショッピング・モールを構築している業者が操作する端末装置を想定し、応答データ以外の情報の発信機能については除外される。

【0013】情報媒介装置2(M)は、情報発信側と情報受信側間の情報通信を媒介する機能を有し、本実施形態に係る機能としてデータ変換部12Aとデータ解釈部12Bとを有する。データ変換部12Aは、ユーザ端末装置1により送信された情報に付加されている送信元アドレスASを、情報媒介装置2自体のアドレスに変換する。データ解釈部12Bは、データ変換部12Aによるデータ変換処理を含めたユーザ端末装置1からのサービス処理の要求内容(ユーザの指示内容)を認識するための機能である。

【0014】情報媒介装置2は、ユーザ端末装置1により送信された情報を受信すると、データ解釈部12Bにより送信情報に含まれる共有データを分離し、この共有データに含まれるサービス処理の要求内容(後述するスクリプト言語により記述された指示内容)を解釈して認識する。さらに、情報媒介装置2は、認識した指示内容に従って、データ変換部12Aによるデータ変換処理と共に、例えば送信に対する情報受信装置3からの応答データをユーザ端末装置1に返信するサービス処理を実行する。

(情報媒介装置2の構成)情報媒介装置2は、図2に示すように、ネットワーク通信処理装置20と、システム制御部21と、データバッファ22と、データ処理部23と、サービス処理部24と、記憶装置25とを有する。ネットワーク通信処理装置20は、ネットワーク回線26に接続して、ユーザ端末装置1と情報受信装置3に対する情報の送受信処理を行なう。データバッファ22は、ユーザ端末装置1や情報受信装置3から受信した情報を格納するためのバッファメモリである。

【0015】システム制御部21、データ処理部23、およびサービス処理部24は、単一または複数のプロセッサ(CPU)から構成されており、本実施形態では便宜的にそれぞれ独立した機能構成要素として取り扱う。記憶装置25は、システム制御部21、データ処理部23、およびサービス処理部24の動作を決定するプログラムを格納しており、それぞれの処理に必要なデータなどを格納するワークメモリの機能も有する。

【0016】システム制御部21は、各構成要素20、22～25を制御すると共に、図1に示すデータ解釈部12Bの機能を有する。ここで、ユーザ端末装置1からの送信情報は、図3に示すように、例えばIP(Internet Protocol)パケット(TCP/IPプロトコルによるIPパケット)形式からなり、送信元アドレスASと宛先(送信先)アドレスADを有するヘッダエリアとデータフィールドからなる。さらに、送信情報は、図4に示すように、大別して本体データDSと、共有データDCと、特定データDPとからなる。本体データDSとは、ユーザ端末装置1から情報受信装置3に送信すべきデータであり、公開性データである。共有データDCは、ユーザ端末装置1と情報媒介装置2とが共有するデータという意味であり、具体的には前述したように、スクリプト言語により記述された指示内容を示すスクリプトデータ、および本体データDSと特定データDPとをアクセスするためのポインタPA、PBからなる。特定データDPは、ユーザにより指定された非公開(または内密)にすべきデータであり、具体的にはユーザの送信元アドレスASを含む。

【0017】システム制御部21は、ユーザ端末装置1からの送信情報から共有データDCを分離して、スクリプトデータを解釈する。この解釈結果により、システム制御部21は、ユーザからの指示内容を認識して、認識結果をデータ処理部23とサービス処理部24に通知する。

【0018】データ処理部23は、システム制御部21からの認識結果に従って、特定データDPに含まれるユーザの送信元アドレスASを情報媒介装置2の送信元アドレスに変換する。また、サービス処理部24は、システム制御部21からの認識結果に従って、ユーザから要求されたサービス処理に対応するアプリケーションプログラムを記憶装置25から呼出し、各種のサービス処理を実行する。

(本実施形態の動作)まず、本実施形態は、ネットワークの利用者であるユーザU(情報発信装置であるユーザ端末装置1)が、例えばネットワーク上に構築されたショッピング・モールのある商店R(情報受信装置3)に対して商品の内容照会を行なう場合を想定する。

【0019】ここで、図6に示すように、本実施形態の情報媒介装置2が介在しない場合には、当然ながらユーザUは、通常のネットワーク・プロバイダなどのネットワーク接続業者を介して、商店Rに対して商品の内容照会を示す情報ISを送信する。商店Rは、その送信情報ISに対する応答データDRをユーザUに送信する。ここで、ユーザUからの送信情報ISには、前述の送信元アドレスASを含む特定データが含まれている。従って、ユーザの個人的なプライベート情報であるアドレスASは、商店R側に知られてしまうことになる。

【0020】そこで、本発明は、情報媒介者M(情報媒

介装置2)を介在させて、いわばユーザからの送信情報ISから非公開したいデータ(アドレスASを含む特定データDP)を除去した送信情報ICを生成して商店Rに転送する。さらに、情報媒介者Mは、商店Rからの応答データDRを受信して、ユーザUに転送するサービス処理を実行する。なお、情報媒介者Mは前記のネットワーク・プロバイダの兼業者や専業業者でもよいし、または他のユーザUが兼ねてもよい。

【0021】以下、図5のフローチャート参照して具体的に説明する。ユーザ端末装置1から情報ISが送信されると、情報媒介装置2はネットワーク通信処理装置20により受信し、データバッファ22に格納する(ステップS1、S2)。システム制御部21は、データバッファ22に格納された送信情報ISから共有データDCを分離し、スクリプトデータの解釈処理を実行する(ステップS3、S4)。即ち、システム制御部21は、スクリプト言語により記述されたユーザUの指示内容(サービス処理の要求を含む)を認識し、データ変換処理の指示があるか否かを判断する(ステップS5)。

【0022】指示内容にデータ変換処理が含まれていない場合、換言すればユーザUから匿名性の確保が要求されていない場合には、システム制御部21は、共有データDC以外の本体データDSと特定データDP(送信元アドレスAS)を含む情報を宛先の商店Rである情報受信装置3に送信する(ステップS6)。

【0023】一方、指示内容にデータ変換処理が含まれている場合には、システム制御部21はデータ処理部23にその旨を指示する(ステップS5のYES)。データ処理部23は、本体データDSと特定データDPとを分離し、特定データDPの送信元アドレスASを情報媒介装置2のアドレス(以下アドレスAMとする)に変換する(ステップS8)。システム制御部21は、変換されたアドレスAMを送信元アドレスとし、宛先アドレスADにより指定された商店Rに対して、共有データDCと特定データDPとを除く本体データDSを含む情報ICを送信する(ステップS9)。

【0024】商店Rである情報受信装置3は、情報媒介者Mを発信先とする本体データDSを受信し、商品の内容照会であることを認識することになる。商店Rは、商品の内容照会に対する応答データ(即ち、照会の商品カタログなどの商品情報)DRを発信先である情報媒介者Mに送信する(ステップS10のYES)。ここで、当然ながらユーザUの送信情報ISが、情報受信装置3からの応答を必要としない内容であれば、情報媒介者Mの処理は終了となる(ステップS10のNO)。

【0025】ここで、ユーザUからのスクリプトデータの中に、応答データの返信処理に関するサービス処理の要求が含まれていれば、サービス処理部24は記憶装置25から該当するアプリケーションプログラムを呼出して実行する。即ち、サービス処理部24は、商店Rから

の応答データDRを受信すると、データバッファ22に保存し、ユーザU側に転送するための処理を実行する(ステップS11, S12)。なお、サービス処理部24は、情報受信R側からの応答処理だけでなく、ユーザUからのスクリプトデータに含まれている各種のサービス処理を実行する。各種のサービス処理の中には、例えばユーザUが複数の商店Rに対して商品の照会をしたときに、各商店Rからの応答データを編集してユーザUに返信する処理や、各種のデータ加工処理(画像処理など)が含まれる。

【0026】さらに、本実施形態は、スクリプトデータの指示により、ユーザが非公開または内密を要求する特定データとして、IPアドレス(ユーザの意思とは無関係に自動的に付加されるデータ)のようないわば属性データを想定したが、これ以外のユーザが指定したデータを特定データとして取り扱ってもよい。

【0027】また、本実施形態では、情報受信側Rがショッピング・モールの商店であり、ユーザUが商品の照会を行なう情報通信を想定したが、当然ながらこれに限ることはない。例えば、ビデオ・オン・デマンドのサービス業者に対して、ユーザUが要望の映像の提供を要請するための情報通信を想定してもよい。このようなサービスでは、情報媒介者MIは、サービス業者から提供される映像情報に対する料金の支払い代行や、提供された映像情報をユーザの要求された時間に送信するようなサービス処理が考えられる。

【0028】以上のように本実施形態によれば、ネットワーク上において、ユーザUが例えば商品の照会などのサービスを要請するための情報を発信したときに、匿名を希望する場合にはその旨を共有データにより指示することにより、発信元を知られることなく情報提供サービスを受けることが可能となる。従って、ユーザUの発信元アドレスなどの個人的なプライバシー情報が、情報媒介者M以外の第3者に対して、意思に反して公開されるようなことを防止することができる。これにより、結果的にユーザのプライバシーを保護すると共に、ユーザの要望する情報提供サービスを実現することが可能となる。

【0029】また、情報媒介者MIは、ユーザUのアドレスと共に、共有データを介して相互の信頼性を確保することにより、情報受信側Rに対するユーザUの信頼性を保証することができる。即ち、情報媒介者MIは、共有データによりスクリプトデータからなるユーザの要求を認識し、かつ本体データや特定データをアクセスすることができる。このため、情報媒介者MIは、必要に応じて外部に対してユーザUの身元などを証明することが可能である。これにより、無制限な匿名性を確保したネットワークシステムとは異なり、発信元であるユーザや送信情報の信頼性を保証することができるため、匿名性を利用したいいわゆるネットワーク犯罪(マネーロンダリングなど)を増長するような事態を防止することが可能であ

る。

【0030】本実施形態では、データ処理部23が、システム制御部21からの認識結果に従って、特定データDPに含まれるユーザの送信元アドレスASを情報媒介装置2の送信元アドレスに変換する構成である。即ち、ユーザの送信元アドレスASを別のアドレス(情報媒介装置2のアドレス)に変換することにより、ユーザの匿名性を確保することが可能となる。

【0031】ここで、コンピュータネットワークに使用される情報通信プロトコルは、例えばインターネットプロトコルとして採用されているTCP/IPプロトコル・モデルのように、複数のレイヤと称する階層化モデルを構成している。この階層化モデルでは、ネットワーク上を転送される情報は、上位層から受けとったIPデータグラムと称する単位情報として取り扱われる。この単位情報は、基本的には図3に示すように、ヘッダエリアとデータフィールドからなる。このとき、このデータフィールドには、階層化モデルでは最上位層に位置する例えば電子メールなどのアプリケーション層において、ユーザにより作成されたメッセージと称する単位情報が含まれている。このメッセージも、基本的には図3に示すように、ヘッダエリアとデータフィールドからなる。従って、ネットワーク上を転送される情報のデータフィールドとは、本実施形態で意味している本体データだけではなく、例えば電子メールなどのアプリケーション層に対応する情報のヘッダエリアが含まれている。

【0032】従って、前記の階層化モデルのような情報通信プロトコルによるネットワーク情報通信では、当然ながら本実施形態のデータ処理部23は、ユーザである情報発信元が識別できるアドレスの全てを別のアドレス(情報媒介装置2のアドレス)に変換する処理を行なうことになる。

(本実施形態の変形例) 本実施形態では、データ処理部23が、システム制御部21からの認識結果に従って、特定データDPに含まれるユーザのアドレスを変換する処理について説明したが、これに限ることなく、データ処理部23はヘッダエリアの全てを変換処理してもよい。換言すれば、情報媒介装置2は、ユーザから受信した情報を再構成して、本体データを除いてヘッダエリアに含まれる全データを変換する。なお、変換後において、ユーザからの送信情報のヘッダエリアに含まれるデータと同一のデータとなるものがある。

【0033】このようなヘッダエリアの全てを変換する処理であれば、以下のような効果がある。即ち、図3に示すように、ヘッダエリアにはアドレスAS, AD以外に、例えば電子メールのメッセージ情報の場合には、発信時刻やサーバ名などのデータBDが含まれている。このようなアドレス以外の他のデータBDにおいても、そのまま情報受信側に送信された場合に、発信元であるユーザを識別または推定できるデータとして利用される可

能性がある。従って、変形例のように、アドレスだけでなく、ヘッダエリアの全てを変換する処理であれば、アドレス以外でユーザの識別可能なデータを所定のデータに変換できるため、ユーザの匿名性の確保をより確実にすることができる。

#### 【 0034 】

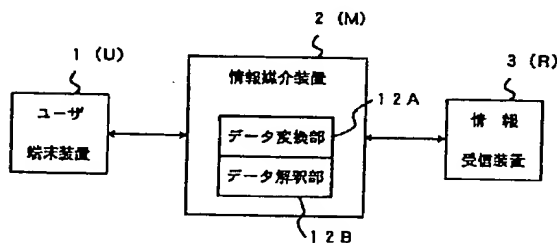
【 発明の効果 】 以上詳述したように本発明によれば、インターネットなどのネットワーク上の情報通信において、情報発信者であるユーザのプライバシー情報が公開されたり、第3者に転送されるなどを防止して、ユーザのプライバシーの保護を図ると共に、ユーザに対して要求された情報提供サービスを行なうことができる。また、同じような電話サービスのような無制限の匿名性を確保した情報通信ではなく、ユーザと発信情報に対する信頼性を保証することができるため、結果的に匿名性を利用したいいわゆるネットワーク犯罪を招くことなく、情報通信の信頼性を保証することが可能である。

#### 【 図面の簡単な説明 】

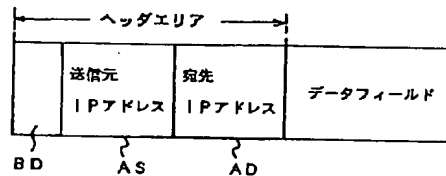
【 図1 】 本発明の実施形態に関するシステム構成を示すブロック図。

【 図2 】 本実施形態に関する情報媒介装置の構成を示すブロック図。

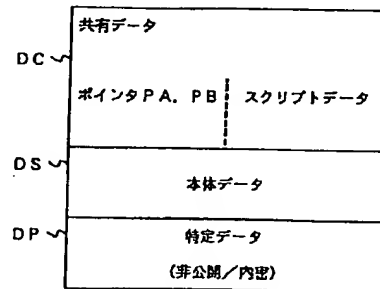
【 図1 】



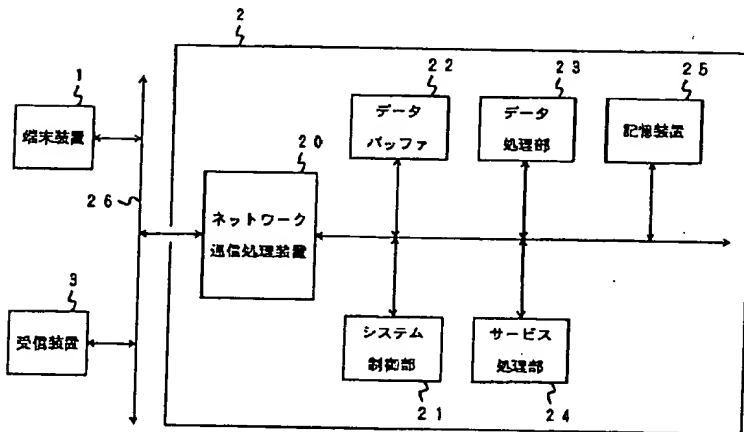
【 図3 】



【 図4 】



【 図2 】



すブロック図。

【 図3 】 本実施形態に関するデータ構造を説明するための概念図。

【 図4 】 本実施形態に関するデータ構造を説明するための概念図。

【 図5 】 本実施形態の動作を説明するためのフローチャート。

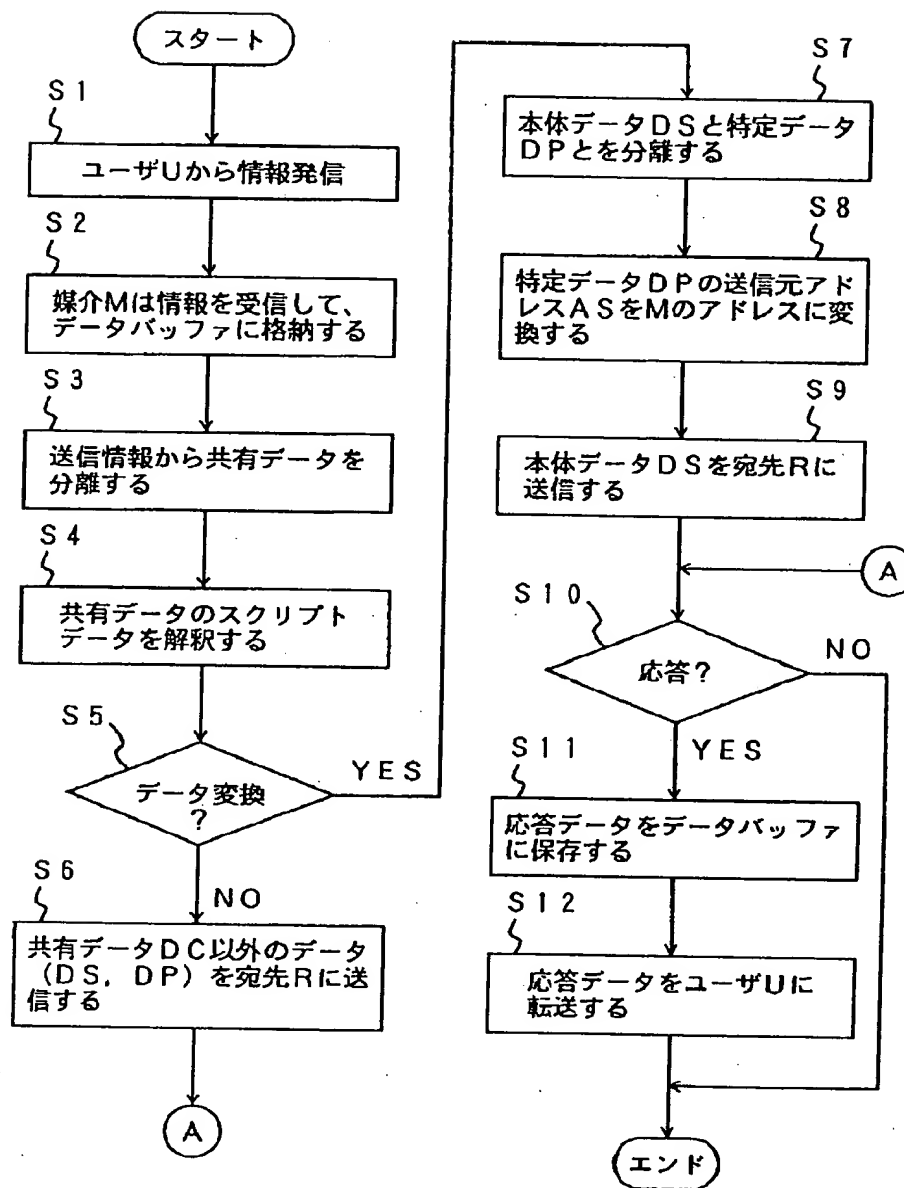
【 図6 】 本実施形態の動作を説明するための概念図。

#### 【 符号の説明 】

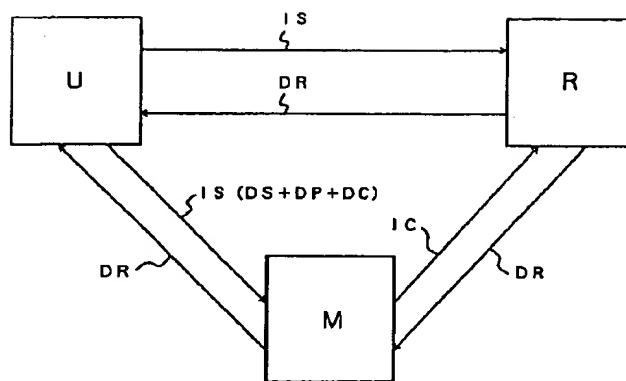
- 1 …情報発信装置(ユーザ端末装置、ユーザU)
- 2 …情報媒介装置(情報媒介者M)
- 3 …情報受信装置(商店R)
- 12A …データ変換部
- 12B …データ解釈部
- 20 …ネットワーク通信処理装置、
- 21 …システム制御部
- 22 …データバッファ
- 23 …データ処理部
- 24 …サービス処理部
- 25 …記憶装置



【 図5 】



【 図6 】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**